Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

<u>**Listing of Claims:**</u>

1. (Currently Amended)   A method of secure communication comprising:

establishing a secure tunnel between ~~first~~ a server and ~~second partie~~ a peer using an encryption algorithm that establishes an encryption key;

authenticating the ~~second party~~ peer with ~~an authentication~~ the server over the secured tunnel establishing an authentication key;

verifying by the ~~first party~~ server that the ~~second party~~ peer possess<u>es</u> the same encryption and authentication keys as the first ~~party~~ server;

provisioning a network access credential to the ~~second party~~ peer using the secured tunnel, responsive to the verifying the ~~second party~~ peer possess<u>es</u> the same encryption and authentication keys as the ~~first party~~ server

<u>signaling an authorization failure to the peer and denying the peer access to the network by the server until the peer authenticates using the provisioned credentials</u>; and

authenticating ~~a second time~~ using a second authentication protocol by the ~~second party~~ peer responsive to the authorization failure, wherein the second authentication is performed using the provisioned network access credential~~;~~

~~wherein access to the second party to the network is denied until the second party successfully authenticates using the provisioned network access credential.~~

2. (Original)   The method of claim 1 wherein the communication implementation between the at least first and second parties is at least one of a wired implementation and a wireless implementation.

3. (Original)   The method of claim 1 wherein the encryption algorithm is an asymmetric encryption algorithm.

4. (Original)   The method of claim 3 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

5. (Original)   The method of claim 3 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

6. (Currently Amended)   The method of claim 1 wherein the step of authenticating the peer is performed using Microsoft MS-CHAP v2.

7. (Original)   The method of claim 1 further comprising a step of provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

8. (Original)   The method of claim 7 wherein the step of provisioning a public/private key pair comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

9. (Currently Amended)   An implementation for enabling secure communication comprising:
    an implementation for establishing a secure tunnel between ~~first~~ server and ~~second parties~~peer using an encryption algorithm that establishes an encryption key;
    an implementation for authenticating the ~~second party~~peer with ~~an authentication~~ server using cryptography with an authentication key;
    an implementation for verifying by the ~~first party~~server that the ~~second party~~peer possesses the same encryption and authentication keys as the first part;
    an implementation for providing a network access credential to the ~~second party~~peer via the secure tunnel responsive to successfully authenticating the ~~second party~~peer and verifying by the ~~first party~~server that the ~~second party~~peer possesses the same encryption and authentication keys;

an implementation for signaling an authorization failure to the peer and denying the peer access to the network by the server until the peer authenticates using the network access credential and

an implementation for ~~performing~~ authenticating using a second authentication protocol, the second authentication protocol is performed using the network access credential~~;~~

~~wherein access to a network is denied until authentication with the network access credential is successful.~~

10. (Currently Amended)   The implementation of claim 9 wherein the implementation for enabling communication between ~~first~~ server and ~~second parties~~peer is at least one of a wired implementation and a wireless implementation.

11. (Original) The implementation of claim 9 wherein the encryption algorithm is an asymmetric encryption algorithm.

12. (Original) The implementation of claim 11 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

13. (Original) The implementation of claim 11 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

14. (Original) The implementation of claim 9 wherein the implementation for authenticating comprises Microsoft MS-CHAP v2.

15. (Currently Amended)   The implementation of claim 9 further comprising an implementation for provisioning a public/private key pair on one of the at least ~~first~~ server and ~~second parties~~peer, and then to provision that public key on the respective remaining ones of the at least ~~first~~ server and ~~second parties~~peer.

16. (Original) The implementation of claim 15 wherein the implementation for provisioning a public/private key pair comprises and implementation for providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

Claims 17 - 25 (Canceled)

26. (Currently Amended)   The implementation of claim 9, that further comprises:

an implementation for hashing the ~~first party~~server encryption key and the ~~first party~~server authentication key to produce a first hash;

an implementation for hashing the ~~second party~~peer encryption key and the ~~second party~~peer authentication key to produce a second hash; and

an implementation for verifying the first and second hash are the same.

Claim 27 (Canceled)

28.   (Currently Amended) The method of claim 1, further comprising invalidating a secure credential for the ~~second party~~peer responsive to a failure of one of the group consisting of establishing the secure tunnel, authentication, and verifying ~~second party~~peer has the same encryption and authentication keys.